BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

暗号と情報セキュリティ

株式会社 昭晃堂

暗号と情報セキュリティ

辻井重男
笠原正雄 編著

定価(本体4,200円＋税)

ISBN4-7856-3075-2 C3055 ¥4200E

$$C=MG'+n \tag{5.76}$$

で与えられる．ここにnはMG'をさらに隠蔽するために付加するベクトルであり，重み$t'\leqq t$のn次元ベクトルである．

受信側においては，まず，

$$CP^{-1}=MSG+nP^{-1}$$

を得る．Pは置換行列であるからnP^{-1}は依然として重みt'のベクトルである．したがってGoppa符号の復号法を用いてnP^{-1}を訂正することによりMSを得ることができる．これより，

$$MSS^{-1}=M$$

として平文Mを復号することができる．このMcEliceの公解謎暗号では行列S, Pの選択に大きな自由度があるほか，Goppa多項式$G(Z)$の選択にもかなりの自由度が存在する．このためMcElice暗号は暗号として安全なものになると考えられている．

参考文献

(1) W. W. Peterson and E. J. Weldon: "*Error-correcting codes*", *Second Ed.*, MIT Press, 1972.

(2) 笠原，田崎，小倉："情報理論—基礎と応用—"，昭晃堂，1985.

6. 認証とディジタル署名

高度情報化社会の出現とともに，通信技術とコンピュータ技術にささえられた情報システムを介して，情報交換が頻繁に行われるようになった．その結果，人間が対面することにより声や姿などから付随的に得られていた個人特有の情報が得られなくなり，情報交換に際して納得して行動することに支障が生じるようになった．情報システムを介して情報交換をしている相手は一体誰なのか，自分が発言した情報はまちがいなく伝えられているか，また，何者かによって故意に改変されていないか．さらには，自分が特定の相手に伝えたつもりの情報は，本当に当人に伝えられたか，などをなんらかの手段により確認する必要がある．このような確認の機能を一般に**認証** (authentication) という．また認証の機能をなんらかのアルゴリズムにより，機械的に実現するシステムを認証システムとよび，その実現手法としては**暗号的手法** (cryptographic scheme) が有効である．したがって本章では暗号的手法を用いた認証とディジタル署名について解説しよう．

6.1 暗号と認証

暗号の機能は大きく分けて，情報の**秘匿** (privacy) と**認証** (authentication) に分類される．情報の秘匿とはなんらかの手段により情報が露呈されることがあっても，鍵がない限りその情報の意味がわからないようにして，第三者に対して情報の機密を守ることである．一方，契約や送金などが伴うビジネスの世界では，署名は欠かせない．電子郵便(electronic mail) や電子送金(electronic funds transfer) といった新しい形態のデータ通信では，文書の署名・捺印に相

当する，情報および送受信者の認証機能を備えていることが，ビジネスの上での争いを避けるためには必要不可欠である．

図 6.1 は暗号の機能を概念的に示したものである．一般に認証と呼ばれている機能は，

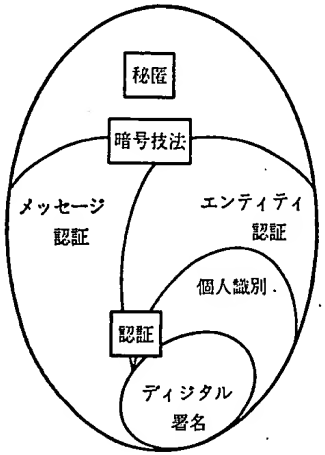


図 6.1 暗号技法の分類

① **メッセージ認証** (message authentication)

② **エンティティ認証** (entity authentication)

および，これら両者の機能を兼ね備えた

③ **ディジタル署名** (digital signature)

に分けられる．

メッセージ認証とは，情報が改変されておらず，原情報のままの正しいものであることを保証する機能である．一方エンティティ認証は，情報システムにおいて情報の生成・伝送・処理・記憶・判断などの行為に関与した実体（エンティティ）Aが，まさにそのエンティティAであることを保証する機能である．すなわち，エンティティAとエンティティBが協調するという条件の下に，AがBにAであることを証明できるが，第三のエンティティCがAになりすまして，Aであることを証明できないことを保証する機能である．

このようなエンティティ認証において“当事者であるエンティティB自身も第三のエンティティCに対して，Aであることを証明できない”という条件を付加するとき，個人識別 (identification) というエンティティ認証の機能になる．

ディジタル署名には，メッセージ認証の機能とエンティティ認証の機能という2面性のあることは，前述の通りである．これをエンティティ認証の見地から見ると，個人識別の機能に“エンティティBがB自身に対してもAであることを証明できない”という条件をさらに付加することにより生まれる新しい機能が，ディジタル署名ということになる．

個人識別とディジタル署名の概念の差異は微妙である．AとBの間でなんらかのトラブルが発生した場合に，Bが問題となっているメッセージの送り主が確かにAであることを証明できる機能が個人識別である．さらにその事実を明示する証拠を呈示することができ，かつBが“にせ”のメッセージを偽造して，“そのメッセージの送り主がAである”と主張することができないとき，そのような機能をディジタル署名という．

図 6.2 はこのような階層構造をもつ3つのエンティティ認証の機能を示している．

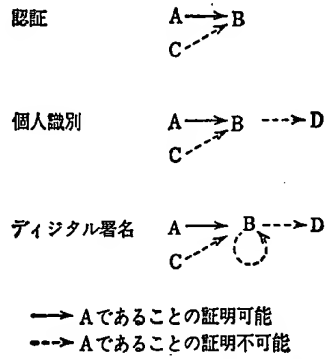
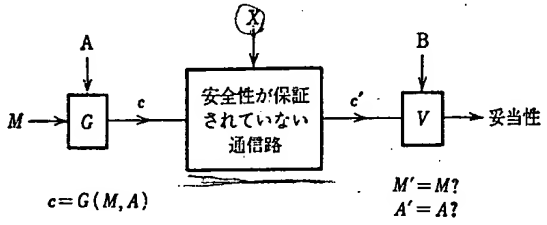


図 6.2 エンティティ認証の階層構造

6.2 認証方式

認証方式の一般概念を図6.3に示す．図中GはメッセージMを通信文cに



A, B：合法的エンティティ　　G：暗号アルゴリズム
X：非合法的エンティティ　　V：認証アルゴリズム

図6.3 認証方式の一般的概念

変換するアルゴリズムであり，Vは受信した通信文c'を認証するアルゴリズムである．AおよびBは情報システムに合法的に関与するエンティティを示し，Xは通信路に介在してメッセージを盗聴したり改ざんしたりする非合法なエンティティ（eavesdropper）を示す．まずAは通信文を生成アルゴリズムGを用いて，メッセージMからcを生成し，必ずしも安全性が保証されていない通信路（insecure channel）を通じてBに伝送する．通信路出力は一般にc'となる．通信文c'を受信したBは認証アルゴリズムVを用いて，復元したメッセージM'とAが送信したメッセージMが等しいかどうか，ならびに受信側のエンティティBが想定している相手が確かにAであるかどうかを検査し，その結果得られる妥当性（validity）を出力する．これが認証方式の一般概念である．

このような一般概念から，図6.4に示すような認証方式を実現する2つの基本形が考えられる．図6.4の（a）は一体型，（b）は分離型と呼ばれている．まず図6.4(a)の一体型では，2つの変換アルゴリズムΓおよびその逆変換Γ^{-1}が，それぞれ鍵K_Γおよび$K_{\Gamma^{-1}}$により制御される暗号化・復号アルゴリズムを形成している．その出力のメッセージM'が意味のあるものであれば，相手のエンティティおよびメッセージが正しいことを認証できる．したがって

認証と同時に秘匿の機能も兼ね備える認証のシステムが構成できる．このような認証方式は通信文復元法と呼ばれている．

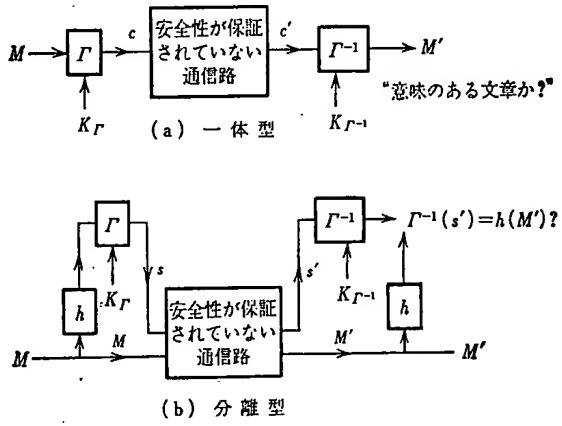


図6.4 認証方式の基本形

図6.4(b)の分離型は，メッセージMを圧縮するなんらかのアルゴリズムが用いられることが特徴であり，普通縮約型のハッシュ関数（hash function）hが用いられる．ΓおよびΓ^{-1}は一体型と同様，鍵K_Γおよび$K_{\Gamma^{-1}}$によって制御される2つの変換アルゴリズムである．またsは認証子（authenticator）とよばれ，受信された認証子s'に復号アルゴリズムΓ^{-1}を適用して得られる値，$\Gamma^{-1}(s')$と受信されたメッセージM'にハッシュ関数を作用させて得られる値$h(M')$が一致するか否かによって，メッセージならびに相手のエンティティを認証できる．このような認証方式は認証子照合法と呼ばれている．

具体的な実現法としては，鍵K_Γおよび$K_{\Gamma^{-1}}$により制御される変換ΓおよびΓ^{-1}に，共通鍵暗号系（common-key cryptosystem）の標準暗号としてよく知られているDES暗号，FEAL暗号などの暗号化・復号アルゴリズムを適用したり，RSA暗号をはじめとする公開鍵暗号系（public-key cryptosystem）の復号アルゴリズムおよび暗号化アルゴリズムを適用する方法が考えられる．ただし共通鍵暗号系を適用する場合には，$K_\Gamma = K_{\Gamma^{-1}} = K$（秘密）であり，公開

鍵暗号系を適用する場合には$K_I=K_D$（秘密），$K_I^{-1}=K_E$(公開）かつ$E_{KE}(D_{KD}(M))=M$が成立しなければならない．

共通鍵暗号系を認証方式の基本形（a）の一体型に適用するとき，実現できる認証システムは，最も制約条件のゆるやかなエンティティ認証とメッセージ認証が同時に実現できる．しかしすべてのメッセージに暗号化および復号処理を施さなければならない．（b）の分離型の場合には，メッセージの秘匿の機能は失われるが，縮約型のハッシュ関数を用いてメッセージMを圧縮しているので，暗号化および復号処理を施すべきデータ量は少なくなる．

公開鍵暗号系を適用した認証システムは，暗号化鍵が公開されているので，後述するようにメッセージの秘匿機能のない認証システムとして位置づけることができる．しかし，暗号化・復号過程を2段にして少し工夫をこらすと，次に述べる最も制約条件の厳しいディジタル署名が実現できる．

6.3 ディジタル署名

6.3.1 公開鍵暗号系を適用したディジタル署名

公開鍵暗号系[1]を認証方式の基本形に適用すると，最も制約条件の厳しいエンティティ認証であるディジタル署名が実現できる．ただし公開鍵K_Eが公開されているので，一体型の認証方式に適用する場合においては，メッセージの秘匿の機能を備えることができない．すなわち，秘密の鍵K_Dを用いてメッセージに暗号化処理を施して伝送しても，その暗号文を盗聴して公開の暗号化鍵K_Eにより容易に平文のメッセージMを得ることができる．前述の通り，一体型の認証システムではすべてのメッセージMに暗号化処理を施すのであるから，もし可能ならば秘匿の機能も兼ね備えたいという要望が発生する．このような要望に的確に答えたディジタル署名方式が存在するので，以下では秘匿の機能を有するディジタル署名方式について述べよう．

公開鍵暗号系の中には暗号化Eと復号Dの順序を交換できる暗号系，すなわち，

$$E_{KE}[D_{KD}(M)]=M \tag{6.1}$$

が支障なく実行できる公開鍵暗号系が存在する．RSA暗号系[2]はその典型的な例である．式（6.1）がなんら支障なく実行できるという前提条件の下に一体型の認証方式を変形して，ディジタル署名と同時に秘匿の機能も備わった認証システムを構成できる．図6.5はエンティティAからエンティティBへ秘密通信を行う場合を想定して構成した秘匿機能を備えた認証システムを示す．こ

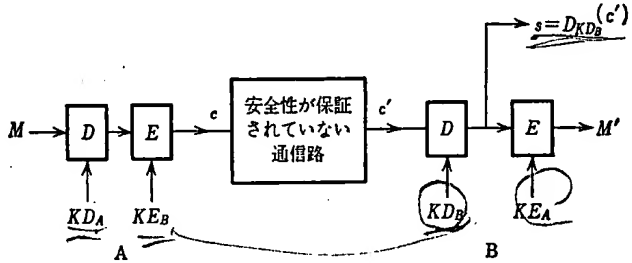


図 6.5 公開鍵暗号系を適用した認証システム

の認証システムの優れている点は，受信側で秘密鍵K_{D_B}を用いてc'を復号した結果得られる値

$$s=D_{KD_B}[c'] \tag{6.2}$$

を取り出せることである．すなわちエンティティAの公開鍵K_{E_A}でsを暗号化することによりメッセージM'が得られるので，もしM'が意味のある平文であれば，そのメッセージ$M'=M$はエンティティAにより送付されたものと断定できる．しかも受信者を含めA以外のいかなるエンティティもこのsを偽造できないので，Bはsを保持することによりAが後でメッセージMを送付した事実を否定できず，制約条件の最も厳しいディジタル署名方式になっている．

公開鍵暗号系を応用したディジタル署名方式を具体的に実現する際には，いろいろな解決すべき問題点が残されている．典型的な公開鍵暗号系としてよく知られているRSA暗号系を用いて実現した場合にも次のような問題がある．

まずRSA暗号系は次のように要約される（詳細は，第3章を参照されたい）．2つの大きな素数p, qをランダムに選び，それらの積$n=pq$を求める．nは公開されるが，2つの素数p, qは秘密に保たれる．次にp, qを用いてnのオイ

ラー関数を，

$$\Phi(n)=(p-1)(q-1) \tag{6.3}$$

により計算する．さらに秘密の$\Phi(n)$により規定される2つの条件

$$\begin{cases} \gcd(d, \Phi(n))=1 & (6.4) \\ \max\{p, q\}<d<\Phi(n) & (6.5) \end{cases}$$

を満たす整数dを任意に選び合同式

$$ed\equiv 1 \mod \Phi(n) \tag{6.6}$$

を解いてeを求める．eは公開鍵として公開リストに登録し，dは秘密鍵として保持する．このような準備の下にエンティティAがエンティティBに秘密にメッセージを伝送する場合，メッセージの1つのブロックを$M(0\leqq M\leqq n-1)$で表現し，公開鍵リストからBの公開鍵$K_{E_B}=(e, n)$を読み取り，暗号文

$$c\equiv M^e \mod n \tag{6.7}$$

を計算してBに伝送する．この暗号文cを受信したBは，秘密鍵$K_{D_B}=(d, n)$を用いて，

$$c^d\equiv M^{ed}\equiv M^{k\Phi(n)+1}\equiv M \mod n \tag{6.8}$$

と計算し，メッセージMを復元する．

このRSA暗号系を図6.5に示す認証システムに適用する場合，エンティティAとエンティティBの使用するn_Aおよびn_Bの値が異なるために，$\mod n_A$と$\mod n_B$の計算の順序の違いにより計算結果が異なるという重要な問題が発生し，具体的な暗号化，復号並びに認証の方法を工夫しなければならない．このような問題に対し，Konfelderが明快な解決法を与えているのでその方法を紹介しておこう．

Konfelder[3]の暗号化および復号の方法は，n_Aとn_Bの大小関係により二つの場合に分けて表6.1のように実行する．

このような暗号通信において，エンティティAとエンティティBの間でなんらかの争いが生じた場合には，調停者の助けを借りて表6.2のような方法で認証することにより解決できる．

表6.1

	$\langle\!\langle n_A<n_B\rangle\!\rangle$	$\langle\!\langle n_A>n_B\rangle\!\rangle$
暗号化	$c=E_{KE_B}[D_{KD_A}(M)]$	$c'=D_{KD_A}[E_{KE_B}(M)]$
復　号	$M=E_{KE_A}[D_{KD_B}(c)]$	$M=D_{KD_B}[E_{KE_A}(c')]$

表6.2

	$\langle\!\langle n_A<n_B\rangle\!\rangle$	$\langle\!\langle n_A>n_B\rangle\!\rangle$
エンティティBが調停者に呈示	$M, x=D_{KD_B}(c)$	M, c'
調停者の計算	$M'=E_{KE_A}(x)$	$\begin{bmatrix} x=E_{KE_B}(M), \\ x'=E_{KE_A}(c') \end{bmatrix}$
判定条件	$M=M'$	$x=x'$

このようなKonfelderの方法では，modulusの大きい方を先に計算し，小さいmodulusによる計算を後で実行するように工夫されている点に着目すると容易に納得できる．またメッセージMは，n_Aとn_Bの小さい方よりも小さくなければならない．

6.3.2 離散対数問題に基づくディジタル署名

ElGamal公開鍵暗号系[4]の提案者として有名なElGamalは，同じ論文の中でElGamal暗号の考え方を応用したディジタル署名方式についても提案している．これは，大きな素数Pを法とする離散対数計算の困難さに基づくディジタル署名方式である．

ElGamalのディジタル署名方式の中心的役割を果たす離散対数問題(discrete logarithm problem)は，次に示すような問題であり，一見簡単そうに見えるが実は極めて困難な問題なのである．いま大きな素数をPとし，Pを法として生成される有限体GF(P)の原始元をαとするとき，方程式

$$y\equiv\alpha^x \mod P \tag{6.9}$$

において，xよりyを求めることは容易であるが，yが与えられたときxを求めることは，極めて困難な問題である．このような一方向性関数を用いて，次のようなディジタル署名方式が実現できる．

エンティティAが署名し，エンティティBが認証する場合を考えよう．まず

準備として，エンティティAは大きな素数Pを選び，これを公開する．また乱数$x_A(0\leqq x_A<P-1)$を生成し，これをAの秘密鍵とする．さらにx_Aとαを用いて，

$$y_A\equiv\alpha^{x_A} \mod P \tag{6.10}$$

を計算し，αとy_Aを公開する．ここでy_Aを公開しても秘密鍵x_Aが割り出せないのは，離散対数問題の困難さに基づいている．

いま署名を行うメッセージをM $(0\leqq M<P-1)$とするとき，次式を満足するrとsの対(r,s)をMの署名とする．

$$\alpha^M\equiv y^r\cdot r^s \mod P \tag{6.11}$$

エンティティAは固有の秘密鍵x_Aを保持しているので，次のようにして署名(r,s)を作成できる．

(i)　$\gcd(k,P-1)=1$および$0\leqq k<P-1$を満たす乱数kを選ぶ．

(ii)　kおよびαを用いて，rを次式により計算する．

$$r\equiv\alpha^k \mod P \tag{6.12}$$

(iii) 式(6.12)を式(6.11)に代入すると，

$$\alpha^M\equiv\alpha^{x_A\cdot r}\alpha^{k\cdot s} \mod P \tag{6.13}$$

となり，

$$M\equiv x_A\cdot r+k\cdot s \mod P-1 \tag{6.14}$$

が得られるので，sについて解くことにより，署名(r,s)が得られる．なおsの一意性は，kが(i)の条件を満たすことにより保証されている．

メッセージMおよび署名(r,s)を受信したエンティティBは，式(6.11)が成立することを確認することにより，Aの署名の正当性を認証できる．

なお，同じkを二度と使用しないように注意しなければならない．なぜならば，異なるメッセージの署名に同じkの値を使用すると，式(6.14)よりx_Aおよびkを未知数とする連立方程式

$$M=x_A\cdot r+k\cdot s$$
$$M'=x_A\cdot r+k\cdot s'$$

が得られ，x_Aが算出できるからである．

6.3.3　ナップザック問題に基づくディジタル署名

MH法と呼ばれているナップザック問題に基づく公開鍵暗号系[5]は，式(6.1)を支障なく実行できるという条件を満足しないために，ディジタル署名には適していない．しかしShamirはナップザック問題のNP完全性に着眼し，MH法を直接適用する方法とは異なった考え方でナップサック問題に基づくディジタル署名法を提案している[6]．

まず簡単に署名の原理を説明しよう．kビットで表現される任意の素数をn，整数表示したメッセージをM $(0\leqq M\leqq n-1)$，1つの正整数ベクトルを$\boldsymbol{a}=(a_1,a_2,\cdots,a_{2k})$とするとき，$M\equiv\boldsymbol{c}\boldsymbol{a} \mod n$，すなわち，

$$M\equiv\prod_{j=1}^{2k}c_ja_j \mod n \tag{6.15}$$

を満足する正整数ベクトル$\boldsymbol{c}=(c_1,c_2,\cdots,c_{2k})$，$0\leqq c_j\leqq[\log_2 n]$を求めるナップザック問題は，NP完全である．ここでナップザック問題の解であるベクトル$\boldsymbol{c}$を署名と考えると，署名の検証は，

$$\boldsymbol{c}\boldsymbol{a} \mod n\equiv M \tag{6.16}$$

によりきわめて容易に実現できる．また署名を偽造するためには，式(6.15)で与えられるNP完全なナップザック問題を解く必要があり，異なるメッセージM'に署名することは，きわめて困難である．

しかし上述の署名の原理によれば，正当な署名者にとっても$\boldsymbol{c}$を計算することは，きわめて困難である．そこでトラップドアとして大きな役割を果たす秘密の情報をk行$2k$列の乱数行列$H=[H_{ij}]$により与え，

$$\begin{bmatrix}h_{1,1} & h_{1.2}\cdots, h_{1,2k}\\ h_{2,1} & h_{2,2}\cdots, h_{1,2k}\\ \cdots\cdots\cdots & \\ \cdots\cdots\cdots & \\ h_{k,1} & h_{k,2}\cdots h_{k,2k}\end{bmatrix}\begin{bmatrix}a_1\\ a_2\\ \cdots\\ \cdots\\ a_{2k}\end{bmatrix}\equiv\begin{bmatrix}2^0\\ 2^1\\ \cdots\\ \cdots\\ 2^{k-1}\end{bmatrix} \mod n \tag{6.17}$$

を満足するベクトル$\boldsymbol{a}=(a_1,a_2,\cdots,a_{2k})$を計算し公開する．上式(6.17)は$2k$

個の未知数を含むk個の方程式であるから，a_1からa_kまではランダムに選ぶことができる．a_{k+1}からa_{2k}まではk個の線形方程式を連立して解くことにより求められる．

いまメッセージをM $(0 \leqq M \leqq n-1)$ とし，Mの2進表現の各ビットを，左側を下位として並べたベクトルを$\boldsymbol{m}$で示すと，メッセージMに対する署名は次式により決定できる．

$$\boldsymbol{c}=\boldsymbol{m}H \tag{6.18}$$

また署名$\boldsymbol{c}$の検証は$\boldsymbol{c}$と$\boldsymbol{a}$を用いて，

$$\begin{aligned}\boldsymbol{c}\boldsymbol{a} \mod n &\equiv \sum_{j=1}^{2k} c_j a_j \mod n \equiv \sum_{j=1}^{2k}\left[\sum_{i=1}^{k} m_i h_{ij}\right] a_j \mod n \\ &\equiv \sum_{i=1}^{k} m_i\left[\sum_{j=1}^{2k} h_{ij} a_j\right] \mod n \equiv \sum_{i=1}^{k} m_i 2^{i-1} \mod n \equiv M\end{aligned} \tag{6.19}$$

となるので，送信されたMとの一致性を確認すればよい．

上述の署名法は完全な方式のように思われるが，数多くのMと$\boldsymbol{c}$の対を集めると上式 (6.18) よりHを決定できる．これを防止するためには，署名する前にメッセージをランダム化すればよい．まずランダムな2進ベクトルを$\boldsymbol{r}=(r_1, r_2, \cdots, r_{2k})$ とし，

$$M^* \equiv (M-\boldsymbol{r}\boldsymbol{a}) \mod n \tag{6.20}$$

を計算する．その結果MはM^*を用いて，

$$M \equiv (M^*+\boldsymbol{r}\boldsymbol{a}) \mod n \tag{6.21}$$

と記述できる．つぎに上述の署名方式を適用してM^*を署名し$\boldsymbol{c}^*$を得る．この$\boldsymbol{c}^*$に$\boldsymbol{r}$を加えて得られる値

$$\boldsymbol{c}=\boldsymbol{c}^*+\boldsymbol{r} \tag{6.22}$$

を署名とする．

署名$\boldsymbol{c}$の検証は次式のようにして容易に実行できる．

$$\begin{aligned}\boldsymbol{c}\boldsymbol{a} \mod n &\equiv (\boldsymbol{c}^*+\boldsymbol{r})\boldsymbol{a} \mod n \\ &\equiv \boldsymbol{c}^*\boldsymbol{a}+\boldsymbol{r}\boldsymbol{a} \mod n \\ &\equiv (M^*+\boldsymbol{r}\boldsymbol{a}) \mod n\end{aligned}$$

$$\equiv M \tag{6.23}$$

このように修正すれば，数多くのMと$\boldsymbol{c}$の対を集めても，行列Hの要素を算出することはきわめて困難になる．

6.4 ID情報に基づくディジタル署名

固有の情報 (identity information, ID) に基づく暗号系と署名法の基本概念は，1984年に開催されたCRYPTO' 84においてShamir[7]により提案された大変興味深いユニークな発想である．この節では，まずID情報に基づく暗号系と署名法の基本概念を示し，次にShamir自身により提案されたディジタル署名法について紹介しよう．

6.4.1 IDに基づく暗号系と署名法の基本概念

送受信者間で公開鍵や秘密鍵を交換する必要が全くなく，また鍵のリストや第三者によるサービスも必要としない方法で，任意のエンティティ間で安全に通信ができ，かつ互いに署名を認証できる新しい暗号化方式である．この方法は信頼できる鍵生成センタの存在を仮定している．鍵生成センタを設置する唯一の目的は，新規にエンティティが情報ネットワークに加入する時に，そのエンティティの名前や住所，電話番号などの固有の情報を受け取り，センタ固有の秘密のアルゴリズムを用いて，そのIDに対応する秘密鍵を生成し，個人ベースで使用するスマートカードに記録して発行することである．このカードの中に収められている秘密の情報により，通信相手が変わっても各エンティティは全く独自に自分の送るメッセージを暗号化したり署名を行うことができる．また自分の受け取る暗号文の復号や認証を行うことができる．IDに基づく暗号系と署名系の概念を図6.6および図6.7に示す．

IDに基づく暗号系と署名法は，公開鍵としてIDを使用し，共通の秘密鍵生成アルゴリズムを鍵生成センタ固有の秘密情報とする，公開鍵暗号方式であると考えられる．